

UNITED STATES DISTRICT COURT
DISTRICT OF RHODE ISLAND

UNITED STATES OF AMERICA

v.

MANISH KUMAR

Criminal Case No 1:20CR89WES-PAS

In Violation of 18 U.S.C. §§ 1343, 1349

INFORMATION

The United States Attorney charges that:

COUNT 1

(Conspiracy to Commit Wire Fraud)

Introduction

At all times relevant to and for the purposes of this Information:

1. Defendant Manish Kumar (“KUMAR”) was a foreign national who held a visa that permitted him to travel and stay for periods of time in the United States.
2. “Pop-up advertisements” refers to the form of online advertising that appears or pops-up suddenly on computer screens while users are browsing other material on the World Wide Web. Generally, pop-up advertisements are generated by code embedded in certain web sites. If a computer user navigates to or from such a web site, the embedded code directs the user’s internet browser to open a new browser window and display the pop-up advertisement.
3. “Malware” refers to software that is designed to disrupt, damage or gain unauthorized access to a computer system. Computer viruses are a form of malware.
4. “Call center” refers to an operation or organization that engages in telephone communications with the public, and includes facilities staffed by operators who attempt to sell purported computer protection services to callers who have been misled to believe that malware has been detected on their computers.
5. “Tech Fraud” refers to a scheme whereby fraudsters mislead victims to believe that malware has been detected on their computers and thereby induce them to part with funds believing that computer protection services are being purchased. To

mislead the victims to believe that malware has been detected on their computers, pop-up advertising is used. To induce the purchase of the purported computer protection services, operators at call centers are used.

6. “Refund Fraud” refers to a scheme whereby funds are obtained from victims of Tech Fraud. The victims are told that they are due refunds, including refunds for purported computer protection services previously purchased. The victims are misled to believe that amounts in excess of the refund amounts are mistakenly deposited in the victims’ bank accounts, even though no deposits are actually made. The victims are thereby induced to direct their own money – falsely characterized as excess funds that were mistakenly deposited – to the fraudsters. Call center operators are used by fraudsters engaged in Refund Fraud.

7. “Money routing” and “account routing” both refer to a money acquisition process, which is used by persons engaged in Tech Fraud and/or Refund Fraud, where fraudsters direct victims to wire money to bank accounts that are held by persons who agree, after receipt, to forward much of the money to the fraudsters.

The Conspiracy

8. Beginning on March 8, 2019 and continuing through August 25, 2019, in the District of Rhode Island and elsewhere, Defendant KUMAR and coconspirators did knowingly, willfully, and unlawfully combine, conspire, and agree with each other and other unknown persons to commit wire fraud by knowingly devising and intending to devise a scheme and artifice to defraud and obtain money and property from others by means of false and fraudulent pretenses, representations, and promises, through the transmission in interstate commerce of wire communications, in violation of 18 U.S.C. §§ 1343.

Object of the Conspiracy

9. The object of the conspiracy was for Defendant KUMAR and his coconspirators to enrich themselves unlawfully by obtaining money from others, including (i) through Tech Fraud by misrepresenting to victims that malware had been detected on their computers and obtaining payment from the victims for putative services that would supposedly remove and manage such malware; (ii) through Refund Fraud by advising victims of Tech Fraud that they would be issued refunds for the amounts paid, misrepresenting that amounts far in excess of the refund amounts had erroneously been deposited into the victims' bank accounts, and thereby inducing the victims to remit the supposed excesses – really the victims' own funds – to Defendant KUMAR and his coconspirators; and (iii) through the unauthorized use of credit card account information to draw funds from victims' credit card accounts.

Manner and Means of Conspiracy

Tech Fraud

10. Via interstate wire transmissions, pop-up advertising was directed – by coconspirators and Defendant KUMAR – to victims falsely representing that malware had been detected on the victims' computers and directing the victims to place telephone calls for assistance.

11. Call routing technology directed the victims' calls to call center operators who offered to sell the victims putative computer protection services and directed them to make payment for those putative services by having funds directed to Defendant KUMAR and coconspirators, including by having victims wire funds to third-party bank accounts.

12. The holders of those third-party accounts, having agreed to provide money routing services to Defendant KUMAR and coconspirators, accepted the victims' wire transfers and then routed much of the wire proceeds, directly or indirectly, to Defendant KUMAR and coconspirators.

Refund Fraud

13. After conclusion of the Tech Fraud, call center operators placed telephone calls to Tech Fraud victims, advised them that they were entitled to refunds, including refunds for the putative services they had purchased. During the interactions, the operators obtained remote access to the victims' computers by suggesting, *inter alia*, that the access was necessary for processing the refunds or conducting a final malware check.

14. Using the remote access, call center operators displayed false account information on the victims' computer screens, and thereby deceive the victims into believing that funds in excess of the supposed refund amounts had been deposited into the victims' bank accounts, even though all the while, no funds were actually deposited into the victims' bank accounts.

15. The call center operators directed the victims to "return" the supposed excess by wiring funds to a specified bank account, a third-party bank account.

16. The holders of those third-party accounts, having agreed to provide money routing services to Defendant KUMAR and coconspirators, accepted the victims' wire transfers and then routed proceeds, directly or indirectly, to Defendant KUMAR and coconspirators.

Credit Card Fraud

17. Through involvement in a mail order operation, Defendant KUMAR and coconspirators received orders by telephone for pharmaceutical products and obtained information sufficient to charge the callers' credit cards, including credit card holders' names, addresses, card numbers, account expiration dates, and card security codes.

18. Defendant KUMAR and coconspirators maintained the credit card information and subsequently sought to obtain money from those credit card accounts by using the card information to place charges on the card accounts by falsely making it appear as though the card holders had made purchases.

Acts in Furtherance of Conspiracy

Account #1 & \$3,500 Sent by LB

19. On or about March 8, 2019, Defendant KUMAR obtained money routing services from AB, and agreed that he and AB would retain and evenly divide amongst themselves a portion of the funds that were routed to the account, the account holder would retain a portion of the funds, and the remainder and majority of the funds would be routed by the account holder to the call center responsible for obtaining the wire transfer.

20. On March 8, 2019, AB sent to Defendant KUMAR a text message containing bank name, account number, routing number, and address for Account #1, a bank account that was to be used for the money routing.

21. On or about March 8, 2019, one of Defendant KUMAR's coconspirator, a call center operator, obtained remote access to LB's computer, offered LB a \$400 refund, and then mislead LB to believe that LB had been issued a \$4,000 refund by mistake, and subsequently LB wired \$3,500 to Account #1, as directed by the coconspirator.

22. Subsequently, on March 8, 2019, Defendant KUMAR via text message sent AB a photograph of an outgoing wire transfer form indicating that \$3,500 had been wired to Account #1 from LB's bank account.

23. Approximately seventeen hours later, Defendant KUMAR via text message to AB inquired about the status of the wire transfer.

Account #2 and \$5,000 Sent by PS

24. On or about August 8, 2019, AB, who was located in Rhode Island, offered to provide money routing services to Defendant KUMAR and sent him a text message containing bank name, account number, routing number, and address for Account #2, a bank account that was used for the money routing.

25. On or about August 9, 2019, one of Defendant's KUMAR's coconspirator, a call center operators, offered PS, who had earlier been led to believe that his computer

had been infected by malware, a refund for previously obtained computer services; obtained remote access to PS's computer; and mislead PS to believe that an amount well in excess of the refund amount had mistakenly been sent to PS's bank account. Subsequently, PS wired \$5,000 to Account #2, as directed by the conspirator.

26. On or about August 9, 2019, Defendant KUMAR via text message sent AB, who was in Rhode Island, a photograph of an outgoing wire transfer form indicating that \$5,000 had been wired to Account #2 from PS's bank account.

27. On August 19, 2019, AB, who was in Rhode Island, received a telephone call from Defendant KUMAR, and he specified that he had a lead on getting \$50,000 but would not be able to pursue that until he received payment for the \$5,000 sent to Account #2.

28. Subsequently, on August 19, 2019, AB, who was in Rhode Island, contacted Defendant KUMAR via text message and requested the "customer id" in case the "bank asked" questions, and Defendant KUMAR responded via text message with PS's name and home address.

Credit Cards

29. On August 12, 2019, Defendant KUMAR texted AB, who was in Rhode Island, credit card information for RG and RW, information that had been collected and compiled with the assistance of other coconspirators and that included account holder name, credit card number, expiration date, and three-digit security code, and Defendant KUMAR specified that the information had been obtained through his "Pharm" business.

30. Subsequently, on August 12, 2019, Defendant KUMAR transmitted to AB a data file containing credit card information for 13 separate credit cards accounts, information that had been collected and compiled with the assistance of other coconspirators and that included the amount previously charged on account for mail order pharmaceutical products and card holder names, addresses, credit card numbers,

expiration dates, and three-digit card security codes.

31. On August 15, 2019, AB, who was in Rhode Island, texted Defendant KUMAR and advised him that attempts had been made to charge small test amounts to some of the credit card accounts but the charges were decline, and Defendant KUMAR responded that those credit card accounts were six months old, specified that they had previously been charged for acquisition of pharmaceuticals, and advised that additional credit card accounts would be transmitted shortly.

32. Subsequently, on August 15, 2019, Defendant KUMAR transmitted to AB two data files containing credit card information for 28 separate credit cards accounts, information that had been collected and compiled with the assistance of other coconspirators and that included the amount previously charged on account for mail order pharmaceutical products and card holder names, addresses, credit card numbers, expiration dates, and three-digit card security codes.

33. Those two date files included the credit card information for RF and TB, both Massachusetts residents, both of whom had within the last year purchased pharmaceutical products online using the credit cards.

34. On August 22, 2019, AB called Defendant KUMAR and advised that two of the credit cards had been successfully charged, and Defendant KUMAR inquired when he would be getting the money. AB asked whether there was any risk of the credit card holders connecting the recent charges to Defendant KUMAR's pharmaceutical business, and Defendant KUMAR responded that he was not concerned because the pharmaceutical charges had occurred about a year ago.

All in violation of 18 U.S.C. § 1349.

COUNTS 2-5
(Wire Fraud)

35. The allegations contained in paragraph 1-7 are re-alleged and incorporated by reference as though fully set forth herein.

Scheme and Artifice to Defraud

36. Beginning on an unknown date that is no later than on or about March 8, 2018 and continuing through August 25, 2019, Defendant KUMAR knowingly and with intent to defraud did devise a scheme to defraud and obtain money from others by means of materially false and fraudulent pretenses, representations, and promises, knowing that they were false and fraudulent when made, through the transmission of wire communications through interstate and foreign commerce.

Object of Scheme to Defraud

37. The object of the scheme to defraud was the same as the object of the conspiracy to commit wire fraud, and accordingly, paragraph 9 is re-alleged and incorporated by reference as though fully set forth herein.

Manner and Means of the Scheme to Defraud

38. The manner and means of the scheme to defraud were the same as the manner and means of the conspiracy to commit wire fraud, and accordingly, paragraphs 10 through 18 are re-alleged and incorporated by reference as though fully set forth herein.

Execution of the Scheme to Defraud

39. On or about the date set forth below, in the District of Rhode Island and elsewhere, for the purpose of executing and attempting to execute the scheme and artifice to defraud, Defendant KUMAR did transmit and cause to be transmitted from abroad and out of state to Rhode Island and elsewhere certain wire communications in interstate and foreign commerce, each wire communication constituting a separate count, as more particularly described below:

COUNT	DATE OF WIRE TRANSMISSION	ACTUAL OR INTENDED AMOUNT	VICTIM IDENTIFIER
2	Mar. 8, 2019	\$ 3,500	LB
3	Aug. 9, 2019	\$ 5,000	PS
4	Aug. 12, 2019	unspecified	Holders of 13 Credit Card Accounts
5	Aug. 15, 2019	unspecified	Holders of 28 Credit Card Accounts

All in violation of 18 U.S.C. §§ 1343 and 1349.

COUNT 6

(Aggravated Identity Theft)

40. On or about August 12, 2019, in the District of Rhode Island and elsewhere, Defendant KUMAR did knowingly transfer and possess, without lawful authority, a means of identification of another person during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), specifically conspiracy to commit wire fraud in violation of 18 U.S.C. 1349 (as charged in Count 1) and fraud in connection with access devices in violation of 18 U.S.C. § 1029, knowing that the means of identification belonged to another actual person,

in violation of 18 U.S.C. § 1028A(a)(1).

COUNT 7

(Aggravated Identity Theft)

41. On or about August 15, 2019, in the District of Rhode Island and elsewhere, Defendant KUMAR did knowingly transfer and possess, without lawful authority, a means of identification of another person during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), specifically conspiracy to commit wire fraud in violation of 18 U.S.C. 1349 (as charged in Count 1) and fraud in connection with access devices in violation of 18 U.S.C. § 1029, knowing that the means of identification belonged to another actual person,
in violation of 18 U.S.C. § 1028A(a)(1).

AARON L. WEISMAN
United States Attorney



MILIND M. SHAH
Assistant U.S. Attorney



SANDRA HEBERT
Assistant U.S. Attorney
Deputy Criminal Division Chief

Date: October 21, 2020